7 способов узнать, кто и чем занимался на компьютере в ваше отсутствие (+бонус)

01.02.2021 | Александр Шихов | Комментарии

Вы вернулись за свое рабочее место и чувствуете, что что-то не так… Монитор стоит под непривычным углом, какие-то крошки на клавиатуре и столе. Вы подозреваете, что кто-то пользовался компьютером в ваше отсутствие? Что же, вполне возможно. Однако доказать вы это не сможете. Или все-таки способ есть? В этой статье я расскажу, как это можно доказать и как поймать с поличным неизвестного.



На самом деле никакая деятельность на компьютере не проходит бесследно. Конечно, если ваш незваный гость не хакер-профессионал. Нет у вас таких знакомых? Тогда начинаем. Начнем с самого простого и постепенно будем углубляться в недра операционной системы.

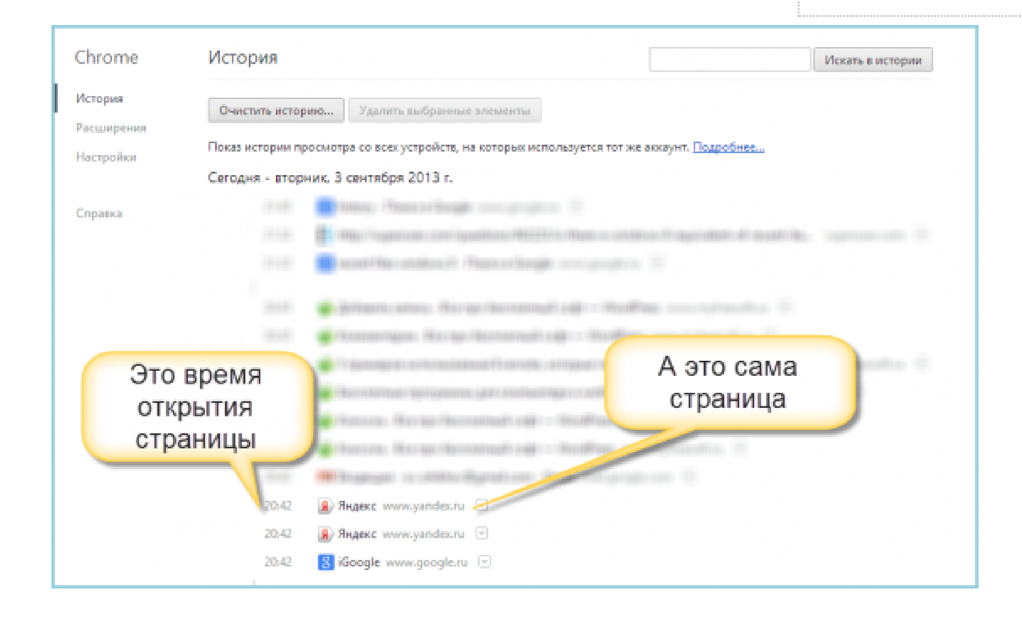
1. Проверяем историю браузеров

Для начала проанализируем историю посещения страниц в Интернете. Эта информация может быть добыта из журналов браузеров, который старательно хранит список всех посещенных сайтов.

Читайте также:

Например, в браузере Google Chrome это делается так. Напишите в строке адреса «chrome://history/» или нажмите сочетание Ctrl-H. Результат представлен на рисунке.

- Как легко очистить историю браузеров и не только



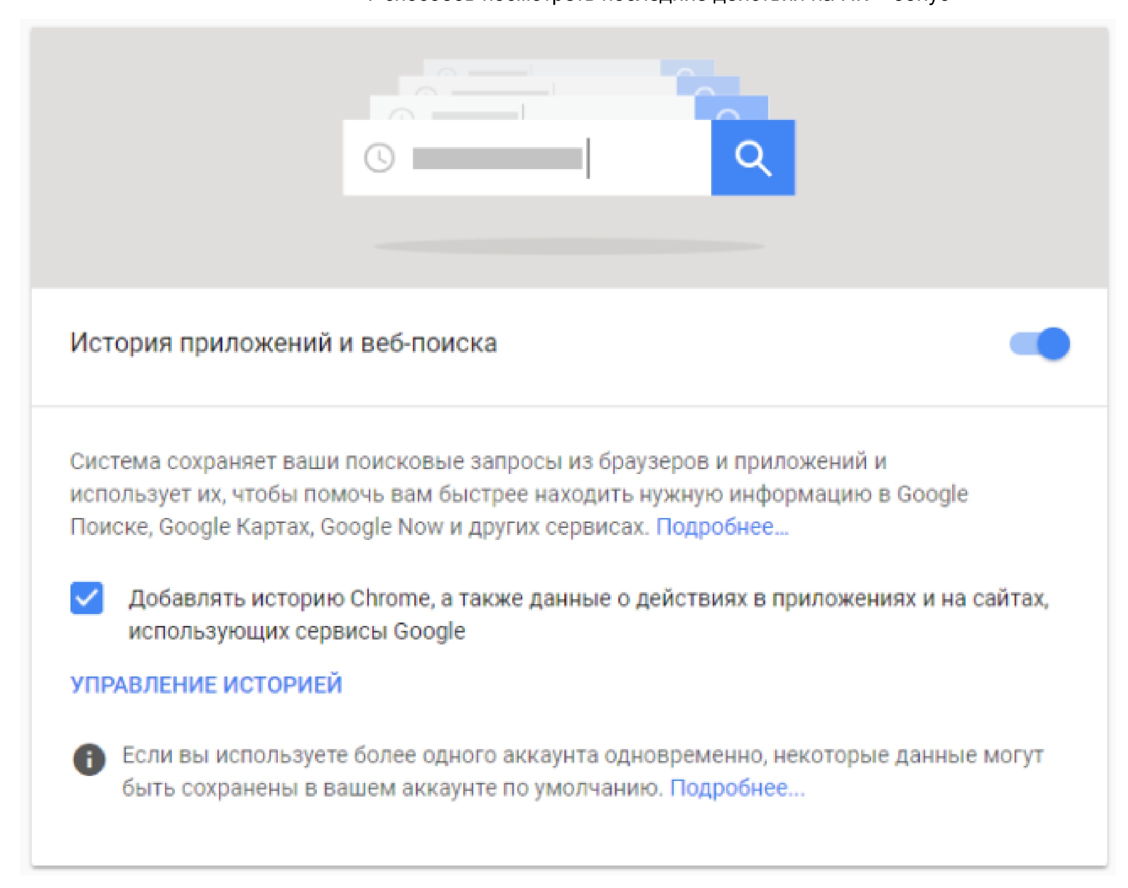
2. Проверяем, что искали в Google

Компания Google очень аккуратно собирает всю историю ваших действий во всех его сервисах и приложениях. И вы, как владелец этих персональных данных, можете проверить всю свою историю в любой момент. Собственно, как и удалить ее, или даже запретить Google сохранять все эти данные.

Среди всей хранимой в Google информации можно найти как поисковые запросы и посещенные сайты, так и открываемые приложения на телефонах.

Смотрите также

- Как избавиться от слежки Google в интернете и за его пределами

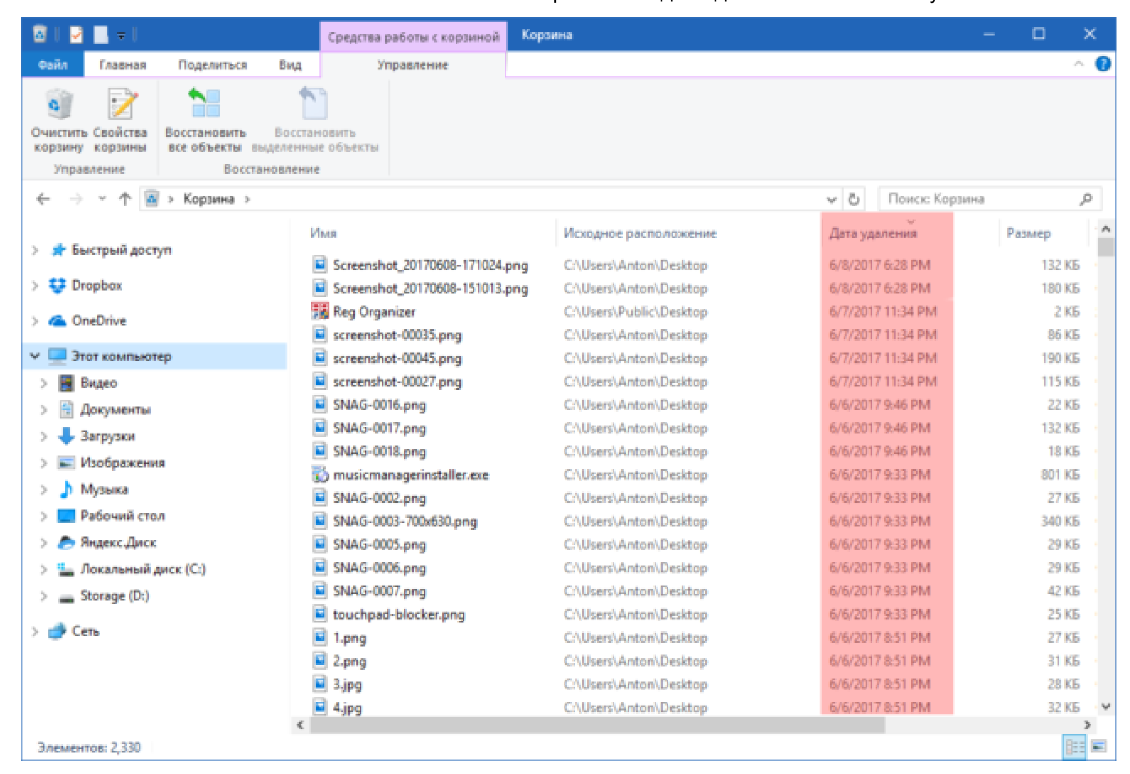


Если кто-то в ваше отсутствие пользовался компьютером и использовал сервисы Google под вашей учетной записью, то вы легко сможете увидеть, что именно просматривалось, куда заходил этот человек, какие поисковые запросы вводил и многое другое.

Найти и изучить всю эту информацию вы можете в специальном разделе «Отслеживание действий».

3. Заглянем в Корзину

Вполне вероятно, что неизвестный мог что-то удалить и забыть при этом очистить Корзину. Во-первых, это позволит понять, что именно было удалено. Во-вторых, позволит восстановить это что-то, если оно важно для вас или представляет какой-то интерес для дальнейшего расследования в изучении действий неизвестного.

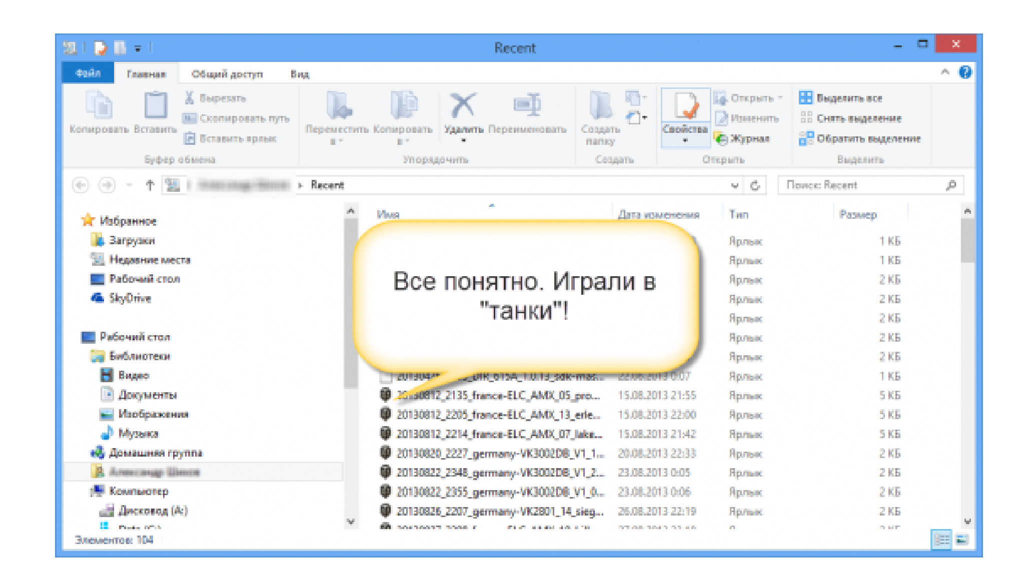


Для этого просто открываем Корзину и сортируем файлы и папки в ней по дате удаления. Просто кликаем по заголовку столбца «Дата удаления» и содержимое сортируется в нужном нам порядке. Ищем интересующий период времени и смотрим, было ли что-то удалено и что именно (если было).

Не исключено, что неизвестный удалил это из Корзины или целиком ее очистил в процессе заметания следов. Но чем черт не шутит, потому лучше всего перепроверить.

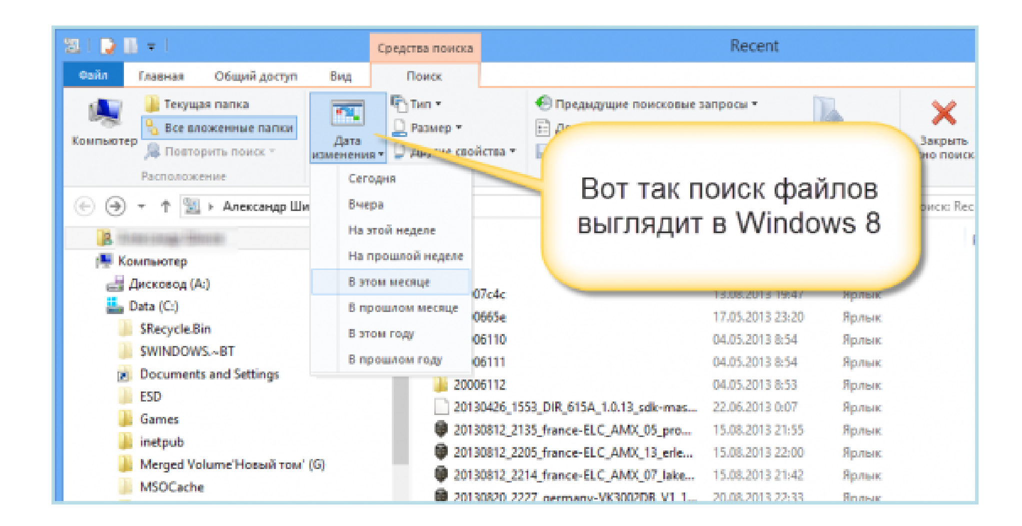
4. Недавно измененные файлы

В меню под кнопкой «Пуск» Windows (кроме Windows 8) есть пункт «Недавние файлы»). Там вы также найдете следы деятельности неизвестного. Чтобы выяснить подобную статистику в Windows 8 придется сделать следующие действия: жмем Win+R, в окне пишем «recent» и нажимаем Enter. Откроется папка недавних файлов.



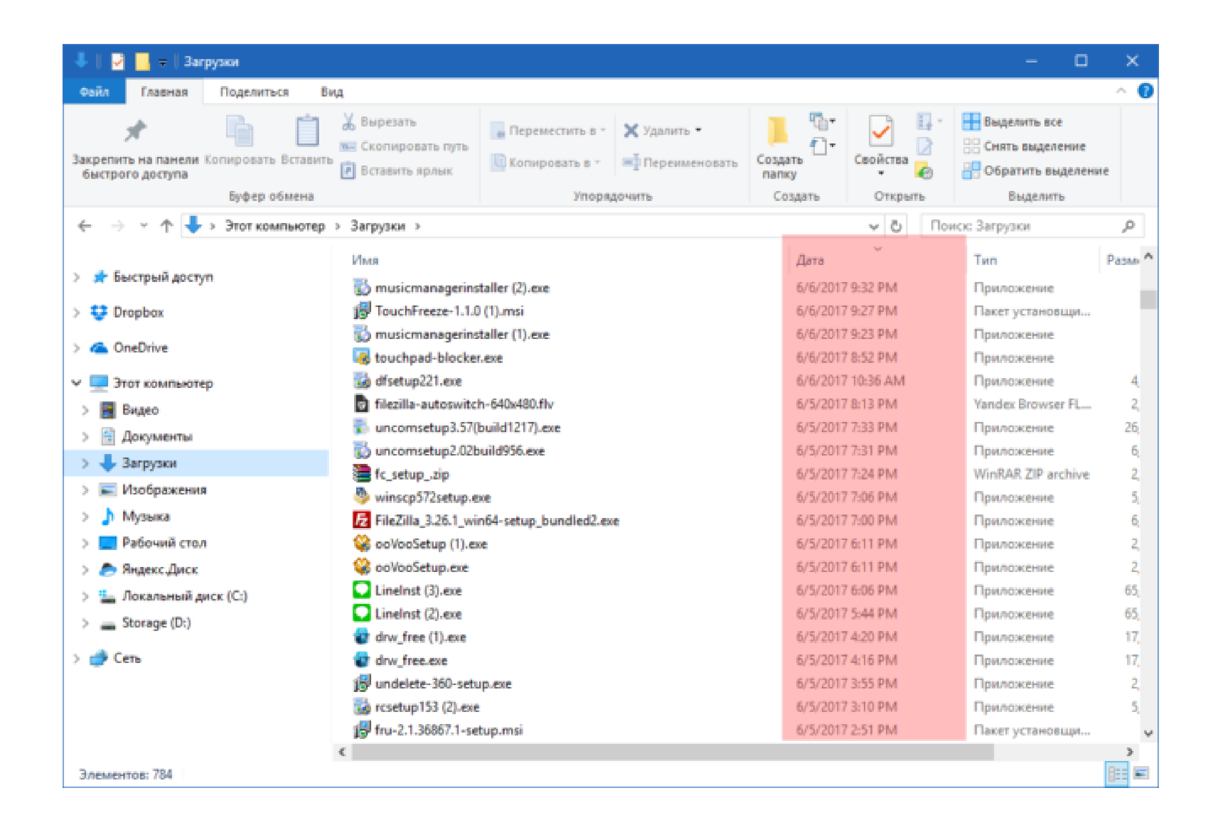
Конечно, может и не повезти, если неизвестный знает о возможности очистить эту папку. Но ее пустота станет еще одним доказательством чужого вмешательства. Ведь вы этого не делали!

Тем не менее, и в случае очистки папки недавних файлов сделать кое-что можно. Откройте Проводник и попробуйте поискать на диске C (можно искать по всем дискам, если у вас их много) файлы с недавней датой изменения.



5. Папка «Загрузки»

Не лишним будет заглянуть в папку «Загрузки» и глянуть, было ли что-то скачено в период вашего отсутствия. Если было, то вы увидите это сразу.

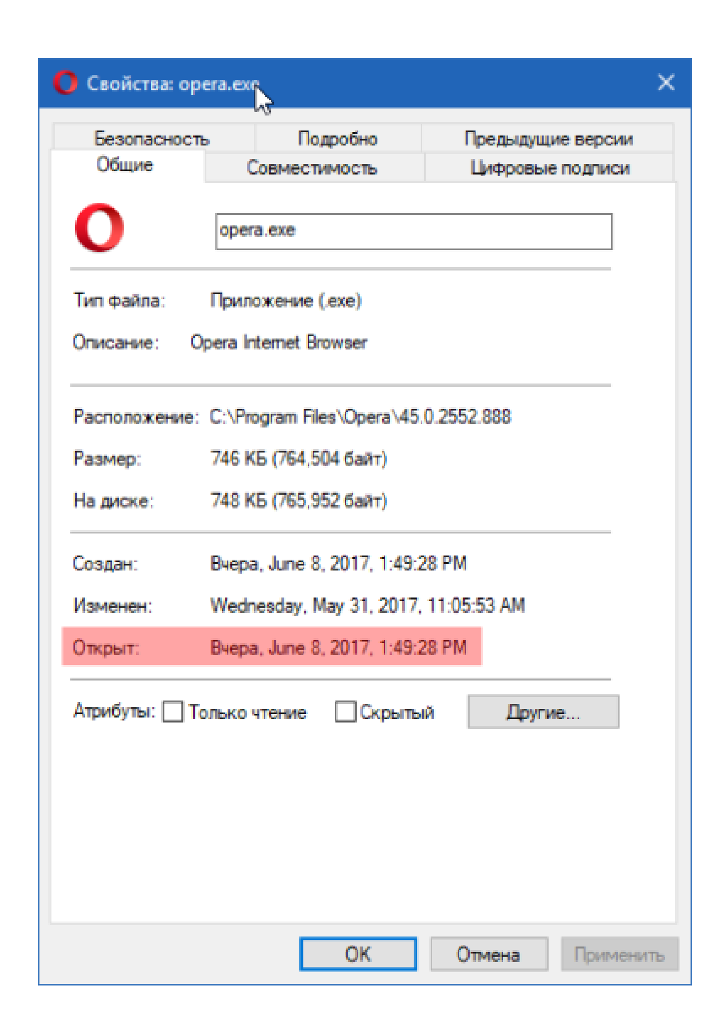


Для этого просто отсортируйте данные по дате создания (столбец «Дата», переключившись предварительно на вкладке «Вид» в редим «Таблица».

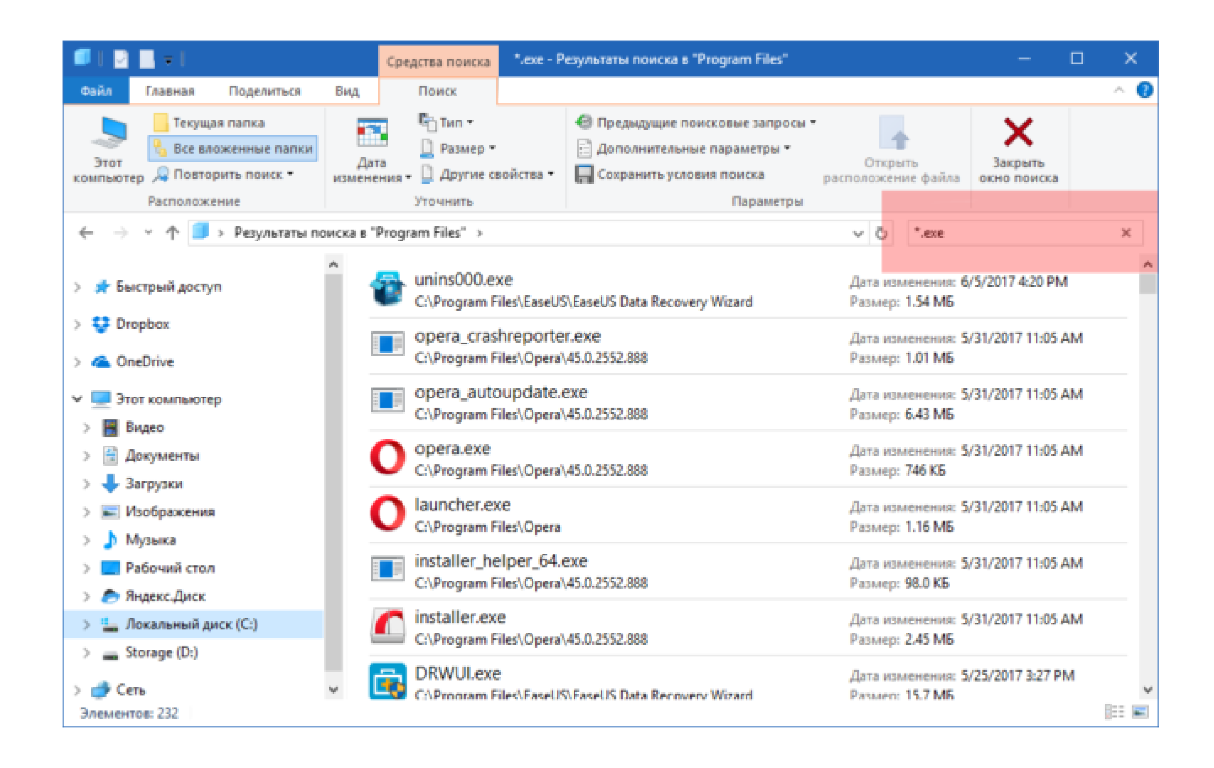
6. Ищем программы, которые запускались в ваше отсутствие

В последних версиях операционной системы Windows (если не ошибаюсь, что начиная с 7 или даже с Vista) среди атрибутов файла имеется поле «Дата открытия». Соответственно, она означает, когда пользователь

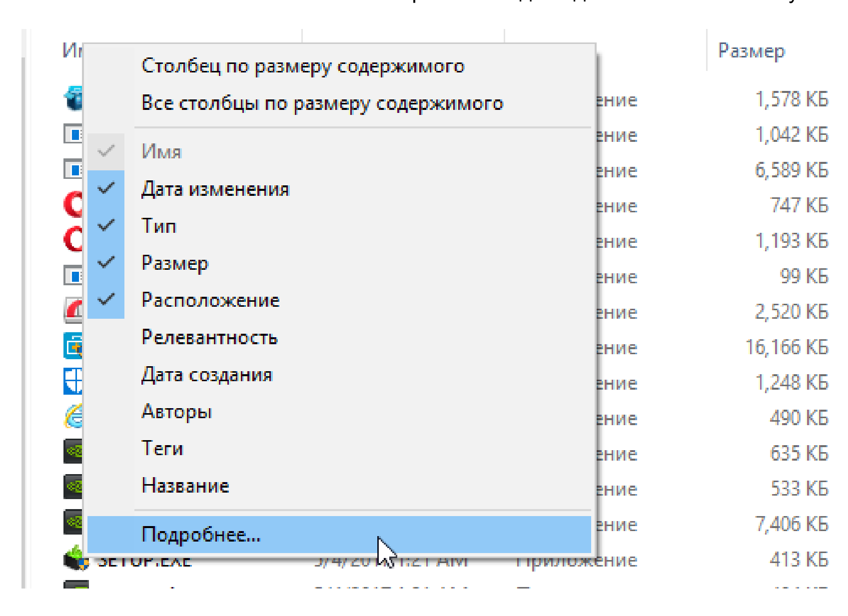
совершил на нем двойной клик и запустил его.



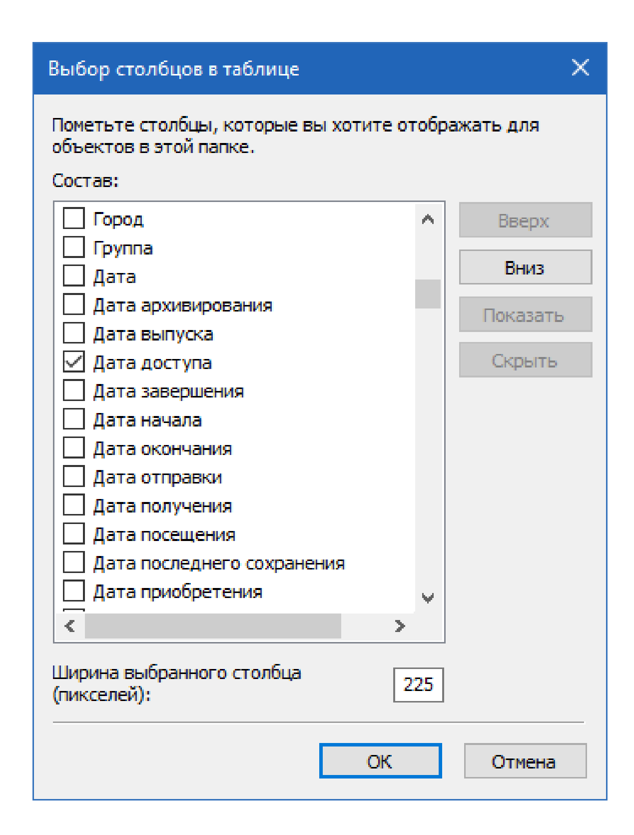
Для этого нам необходимо найти все программы. Запускаем Проводник и заходим в папку «C:\Program Files\», в правом верхнем углу в поле для поиска вводим поисковой запрос «*.exe» и жмем Enter.



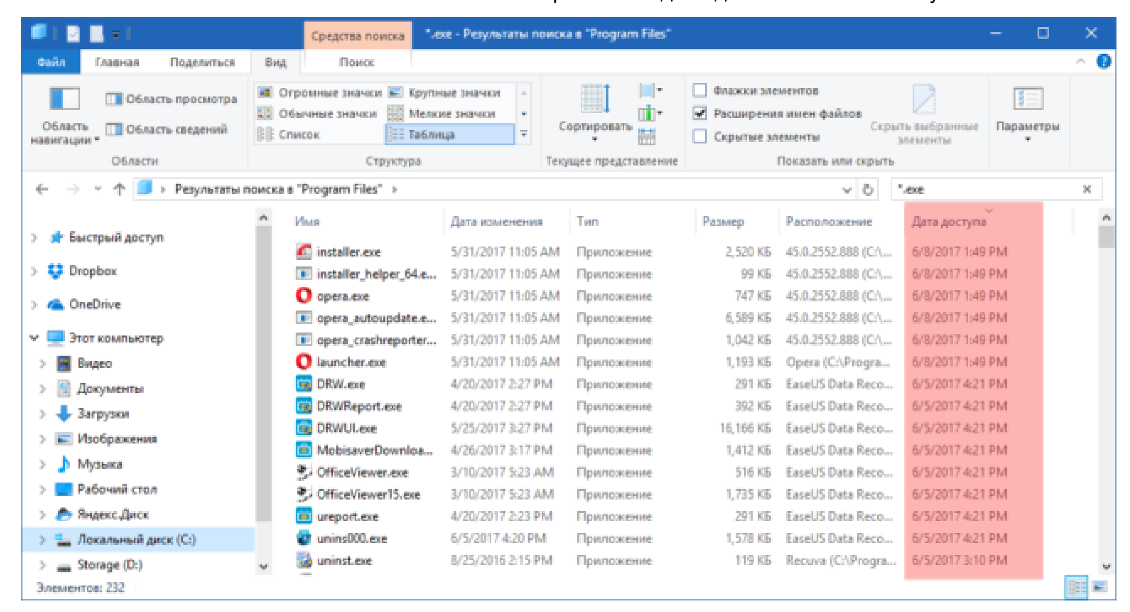
В списке начнут появляться исполняемые файлы, которые находятся в этой папке.



Нам нужно на вкладке «Вид» переключиться в режим «Таблица». Затем кликнуть по заголовку любого столбца правой кнопкой мышки и в появившемся меню выбрать пункт «Подробнее…».



В появившемся маленьком окошке ищем пункт «Дата доступа», устанавливаем напротив него галочку и жмем ОК.



Остается кликнуть по заголовку столбца «Дата доступа» и найти интересующий период времени, когда предполагаемый неизвестный что-то делал на компьютере.

Если вы используете 64-разрядную версию Windows, то у вас будет еще одна папка — «C:\Program Files (x86)\». С ней нужно проделать то же самое.

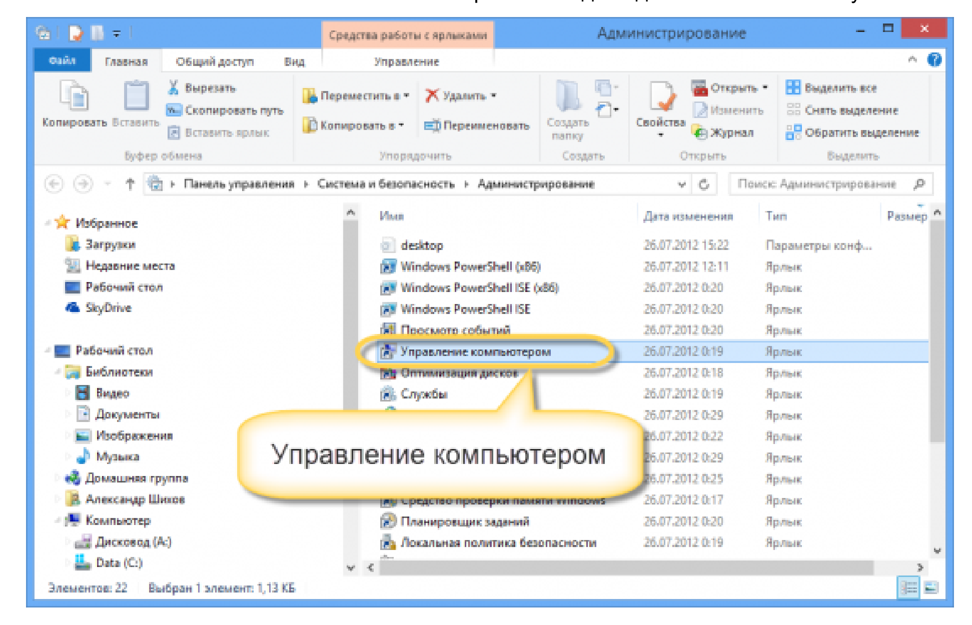
Также не забывайте о папке с играми, если они установлены в другом месте (например, на другом диске). Так стоит проделать те же действия. Ну и, конечно же, если у вас есть еще где-то установленные программы, то стоит заглянуть туда тоже.

> ***Обратите внимание!*** *Если вы с момента включения компьютера запускали какие-либо приложения, то данные о предыдущем запуске будут удалены. Если неизвестный запускал ранее те же приложения, что запустили вы после него, то в свойствах файла этих приложений будет дата вашего запуска. Дату предыдущего запуска узнать будет уже нельзя в данном случае.*

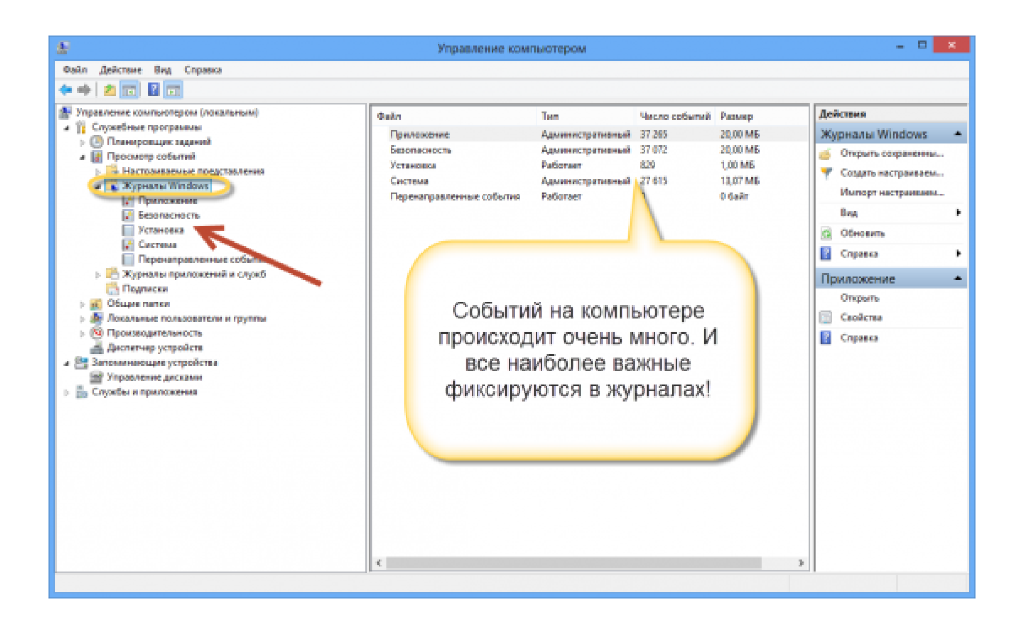
7. Анализируем файлы журналов

Журналы Windows содержат довольно много информации о работе пользователей, ходе загрузки операционной системы и ошибках в работе приложений и ядра системы. Вот туда мы и заглянем в первую очередь.

Откройте «Панель управления» (Control Panel), найдите пункт «Администрирование» (Administrative Tools) и выберите «Управление компьютером» (Computer Management).

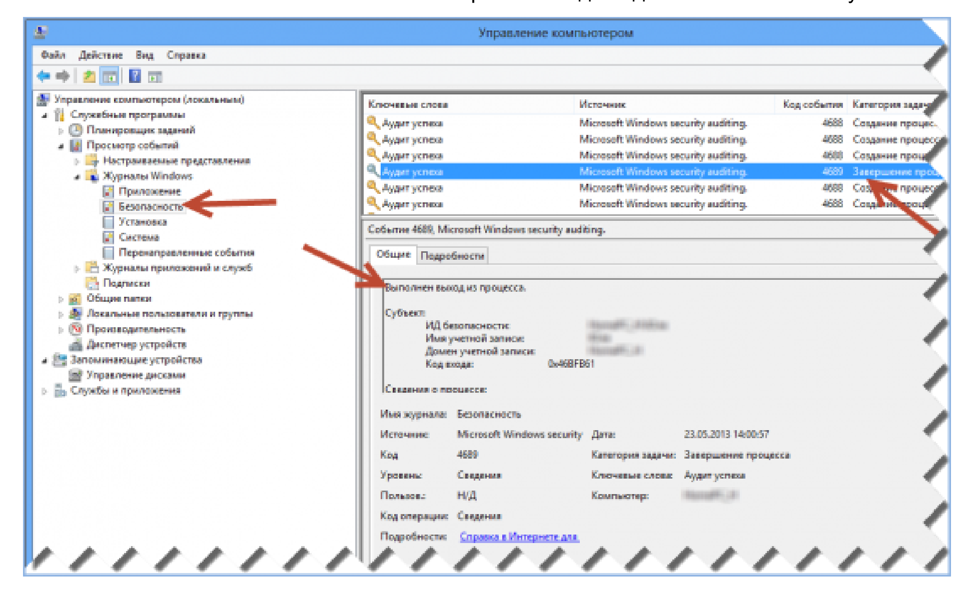


Здесь вы увидите «Просмотр событий» (Event Viewer) в левой навигационной панели. Вот в этом пункте меню и находятся «Журналы Windows». Их несколько: Приложение, Безопасность, Установка, Система.



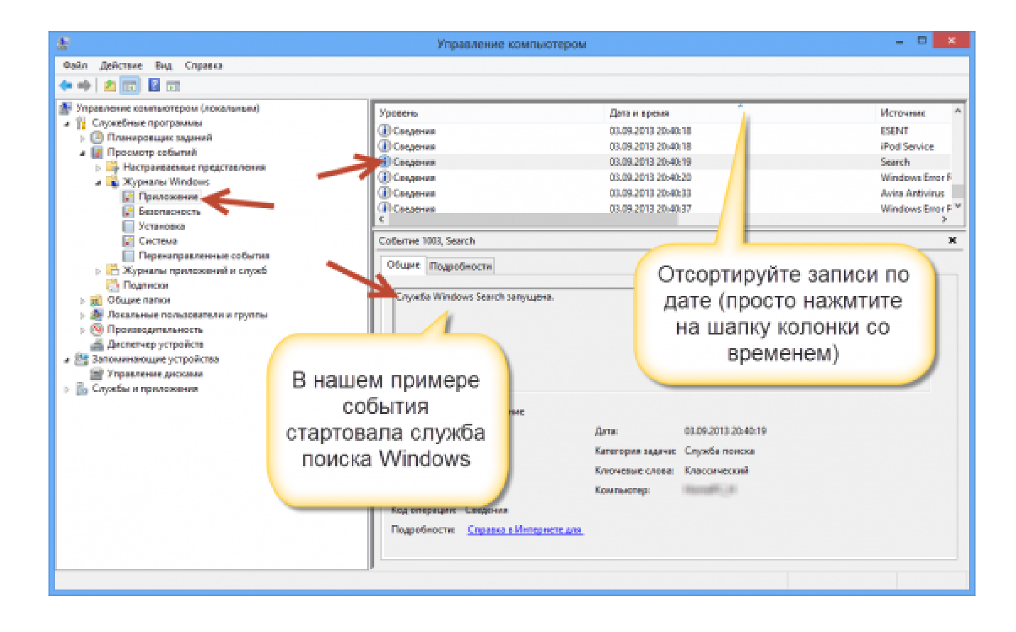
Журнал безопасности

Нас сейчас больше всего интересует журнал безопасности. Он обязательно содержит информацию о входе в систему всех пользователей. Найдите запись о вашем последнем выходе из системы. А все записи журнала, которые будут расположены между вашим последним выходом и сегодняшним входом — это следы деятельности другого лица.



Журнал приложений

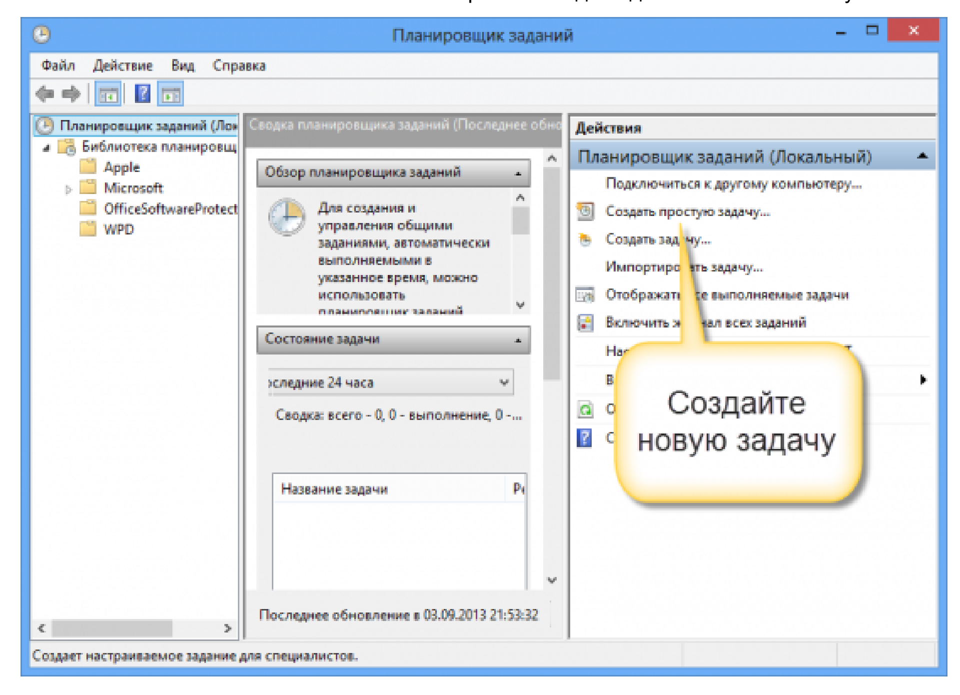
Теперь перейдем к журналу приложений. Он тоже очень важен для нашего маленького расследования. Этот журнал содержит информацию о приложениях, которые были запущены в наше отсутствие. Для подтверждения факта, что не вы эти приложения запускали, ориентируйтесь на время события.



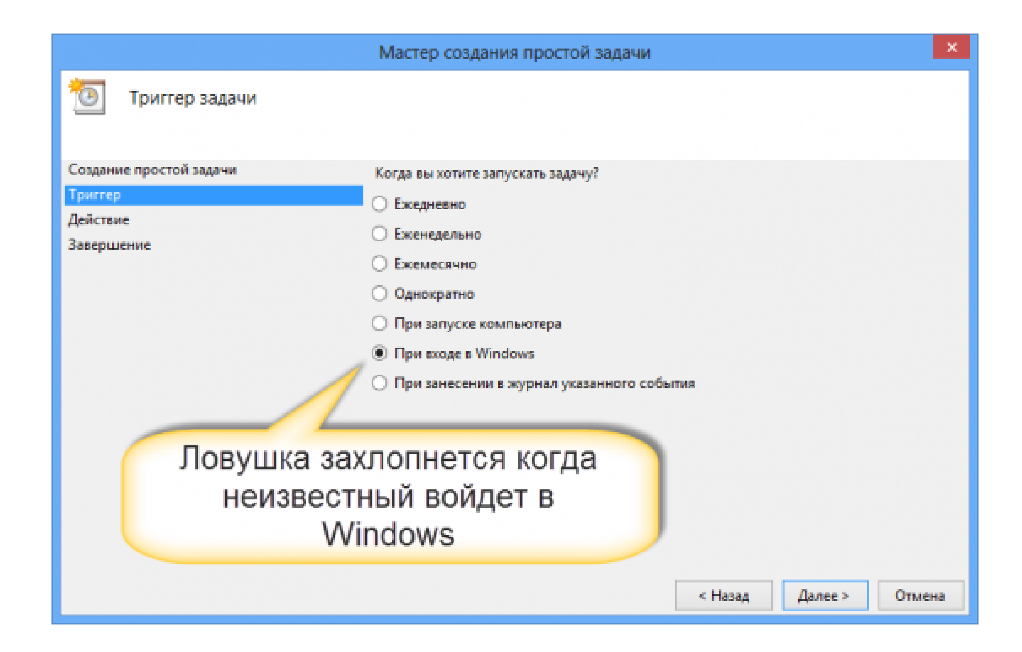
Итак, анализируя два этих журнала, вы точно определите не только сам факт входа под вашим именем в ваше отсутствие, но и определите приложения, которые запускал этот неизвестный.

[Бонус] Ставим ловушку для неизвестного

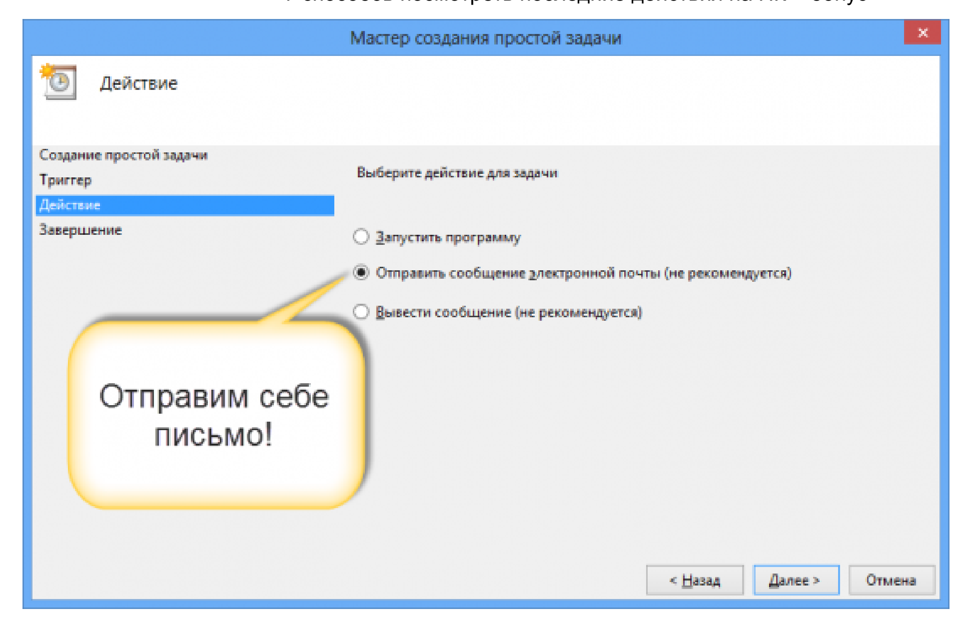
Вот теперь, имея все доказательства на руках, мы можем предположить, кто использует наш компьютер и поговорить с ним. Но еще лучше взять его с поличным! Для этого можно использовать штатный Планировщик задач Windows.



При создании задачи укажите событие (триггер) «Вход в Windows».



Теперь продумайте, что вы бы хотели сделать, когда без вас кто-то войдет в компьютер. Самый простой вариант — послать самому себе письмо, например, на коммуникатор.



Хотя лично мне больше понравился бы вариант «Запустить программу». А потом бы я скачал какую-нибудь программу-розыгрыш из тех, что переворачивают экран или вызывают его «осыпание». Представьте себе лицо неизвестного в этот момент!